

10 MAR 1989

CHAPTER 4

SECURITY EDUCATION

4-1 BASIC POLICY

1. Each command handling classified information will establish and maintain an active security education program to instruct all personnel, regardless of their position, rank or grade, in security policies and procedures.

2. The purpose of the security education program is to ensure that all personnel understand the need and procedures for protecting classified information. The goal is to develop fundamental security habits as a natural element of each task.

4-2 RESPONSIBILITY

1. CNO (N09N) is responsible for policy guidance, education requirements and support for the DON security education program. Development of security education materials for use throughout the DON must be coordinated with CNO (N09N2) for consistency with current policies and procedures. This requirement does not apply to materials which are prepared for use in command programs.

2. Recruit training commands are responsible for indoctrinating military personnel entering the Navy and Marine Corps, with a basic understanding of what "classified information" is and why and how it is protected. Civilians being employed by the DON for the first time (who will handle classified material) must also be given a basic security indoctrination by the employing activity.

3. Commanding officers are responsible for security education in their commands, ensuring time is dedicated for training and awareness. Supervisors, in coordination with the command security manager, are responsible for determining security requirements for their functions and ensuring personnel under their supervision understand the security requirements for their particular assignment. On-the-job training is an essential part of command security education and supervisors must ensure that such training is provided.

4-3 SCOPE

1. Security education must be provided to all personnel. The education effort must be tailored to meet the needs of the command, as well as those of different groups within the command.

10 MAR 1988

2. In formulating a command security education program, the security manager must provide for the minimum briefing requirements of this regulation. Security managers must guard against allowing the program to become stagnant or simply comply with requirements without achieving the real goals.

3. The security education program should be developed based on the command mission and function and should:

a. Advise personnel of the adverse effects to the national security which could result from unauthorized disclosure of classified information and of their personal, moral and legal responsibility to protect classified information within their knowledge, possession or control;

b. Advise personnel of their responsibility to adhere to the standards of conduct required of persons holding positions of trust and to avoid personal behavior which could render them ineligible for access to classified information or assignment to sensitive duties;

c. Advise personnel of their obligation to notify their supervisor or command security manager when they become aware of information with potentially serious security significance regarding someone with access to classified information or assigned to sensitive duties;

d. Advise supervisors of the requirement for continuous evaluation of personnel for eligibility for access to classified information or assignment to sensitive duties;

e. Familiarize personnel with the principles, criteria and procedures for the classification, downgrading, declassification, marking, control and accountability, storage, destruction, and transmission of classified information and material and alert them to the strict prohibitions against improper use and abuse of the classification system;

f. Familiarize personnel with procedures for challenging classification decisions believed to be improper;

g. Familiarize personnel with the security requirements for their particular assignments and identify restrictions;

h. Instruct personnel having knowledge, possession or control of classified information how to determine, before disseminating the information, that the prospective recipient has been authorized access, needs the information to perform his/her

10 MAR 1988

official duties, and can properly protect (store) the information;

i. Advise personnel of the strict prohibition against discussing classified information over an unsecured telephone or in any other manner that may permit interception by unauthorized persons;

j. Inform personnel of the techniques employed by foreign intelligence activities in attempting to obtain classified information;

k. Inform personnel of their particular vulnerability to compromise during foreign travel;

l. Advise personnel that they are to report to their commanding officer, activity head or designee, contacts with any individual regardless of nationality, whether within or outside the scope of the individuals official activities, in which:

(1) illegal or unauthorized access is sought to classified or otherwise sensitive information; or

(2) the employee is concerned that he or she may be the target of exploitation by a foreign entity.

m. Advise personnel of the penalties for engaging in espionage activities and for mishandling classified information or material.

4-4 MINIMUM REQUIREMENTS

1. The following are the minimum requirements for security education:

a. Indoctrination of personnel upon employment by the DON in the basic principles of security (paragraph 4-5 applies).

b. Orientation of personnel who will have access to classified information at the time of assignment, regarding command security requirements (paragraph 4-6 applies).

c. On-the-job training in specific security requirements for the duties assigned (paragraph 4-7 applies).

d. Annual refresher briefings for personnel who have access to classified information (paragraph 4-8 applies).

SECNAVINST 5510.30A

10 MAR 1998

e. Counterintelligence briefings once every 2 years for personnel who have access to information classified Secret or above (paragraph 4-9 applies).

f. Special briefings as circumstances dictate (paragraph 4-10 applies).

g. Debriefing upon termination of access (paragraph 4-11 applies).

4-5 INDOCTRINATION

1. Personnel entering employment with DON need to have a basic understanding of what classified information is, and the reasons(s) for its protection, as well as how to protect it.

2. A basic indoctrination for military members is done during training at the time of accession. Civilians will be indoctrinated by the employing command.

3. Through indoctrination, all personnel should know that:

a. Certain information, essential to the national security, requires protection from disclosure to unauthorized persons;

b. Classified material will be marked to show the level of classification;

c. Only those who have been officially and specifically authorized may have access to classified information;

d. Personnel will be continually evaluated regarding their eligibility to access classified information and to be assigned to a sensitive position.

e. Classified material must be stored and used in secure areas, must be protected during transfer from one area to another (including electronic transfer), and must be destroyed by authorized means;

f. Any compromise or other security violation must be reported;

g. Any attempt by an unauthorized person, regardless of nationality, to solicit classified information must be reported.

10 MAR 1990

4-6 ORIENTATION

1. Personnel who will have access to classified information will be given a command security orientation briefing as soon as possible after reporting aboard or being assigned to duties involving access to classified information.

2. A review of written command security manuals or material is not normally considered to provide an adequate orientation.

3. The timing and format for orientation will vary, depending on the size of the command. At large commands with a high turnover rate, briefings may be scheduled on a regular basis. At smaller commands, with irregular changes of personnel, individual instruction may be necessary.

4. Through orientation, all personnel should know:

a. The command security structure (i.e., who the security manager is, who the TSCO is, SSO, etc.);

b. Any special security precautions within the command, (e.g. restrictions on access);

c. Command security procedures for badging, security checkpoints, destruction, visitors, etc.;

d. Their responsibility to protect classified information;

e. Their obligation to report suspected security violations;

f. Their obligation to report information which could impact on the security clearance eligibility of an individual who has access to classified information;

5. The security orientation should be tailored to the command and to the individual receiving it. More emphasis on security procedures will be needed when the individual has not had previous experience handling classified information.

4-7 ON-THE-JOB TRAINING

1. On-the-job training is the phase of security education when security procedures for the assigned position are learned. Security managers will assist supervisors in identifying appropriate security requirements.

2. Supervision of the on-the-job training process is critical. Supervisors are ultimately responsible for procedural violations or for compromises which result from improperly trained personnel. Expecting subordinates to learn proper security procedures by trial-and-error is not acceptable.

4-8 REFRESHER BRIEFINGS

1. Once a year, all personnel who have access to classified information will receive a refresher briefing designed to enhance security awareness.

2. The refresher briefing may be addressed to the entire command or it could be tailored for particular groups in the command. It should cover general security matters but need not cover the whole subject of security.

3. Refresher briefings should cover:

- a. New security policies and procedures,
- b. Counterintelligence reminders regarding reporting contacts and exploitation attempts and foreign travel issues;
- c. Continuous evaluation;
- d. Command specific security concerns or problem areas. Results of self-inspections, inspector general reports, or security violation investigations provide valuable information for use in identifying command weaknesses.

4-9 COUNTERINTELLIGENCE BRIEFINGS

Once every 2 years in accordance with SECNAVINST 5520.3B, Criminal and Security Investigations and Related Activities Within the Department of the Navy, 4 Jan 93, those who have access to material classified Secret or above must be given a counterintelligence briefing by an NCIS agent. The security manager is responsible for arranging for the briefing with the local NCIS office.

4-10 SPECIAL BRIEFINGS

Briefings not required as a matter of routine, but which may be governed by circumstances or other program requirements are considered special briefings and may include the following:

10 MAR 1988

1. Foreign Travel Briefing

a. Although foreign travel (personal or business) may be briefly discussed during annual refresher briefings, it may also be appropriate to require separate foreign travel briefings for personnel, especially for those who travel frequently. It is in the best interest of the command and the traveler to ensure travelers are fully prepared for any particular security or safety concerns that the foreign travel may introduce.

b. A foreign travel briefing is usually only offered to those individuals who have access to classified information. However upon request, an unclassified version may be given to dependents, or others who do not have access, separately. (Individuals with SCI access should be referred to their SSO for foreign travel briefing requirements).

c. Upon return of the traveler, they should be provided the opportunity to report any incident - no matter how insignificant it might have seemed - that could have security implications.

d. Audiovisual material for a formal foreign travel briefing is stocked at servicing NCIS offices.

2. New Requirement Briefings. Whenever security policies or procedures change, personnel whose duties would be impacted by these changes must be briefed as soon as possible.

3. Program Briefings. Briefings that are specified or required by other program regulations (e.g. NATO, SIOP-ESI, SCI, etc.)

4-11 COMMAND DEBRIEFING

1. A debriefing will be given to individuals who no longer require access to classified information as a result of:

a. Transfers from one command to another;

b. Terminating active military service or civilian employment;

c. Temporarily separating for a period of 60 days or more, including sabbaticals, leave without pay status, or transferred to the Inactive Ready Reserves (IRR);

d. Expiration of a Limited Access Authorization (LAA);

SECNAVINST 5510.30A

10 MAR 1990

e. Inadvertent substantive access to information which the individual is not eligible to receive;

f. Security clearance eligibility revocation; or

g. Administrative withdrawal or suspension of security clearance and SCI access eligibility for cause. Refer to reference (c) for additional information.

2. Debriefings must include the following:

a. All classified material in individuals' possession must be returned;

b. Individuals are no longer eligible for access to classified information;

c. Reminder of provisions of the Classified Nondisclosure Agreement (SF 312) to never divulge classified information, verbally or in writing, to any unauthorized person or in judicial, quasi-judicial, or in administrative proceedings without first receiving written permission of CNO (N09N);

d. There are severe penalties for disclosure; and

e. The individual must report to the NCIS (or to the FBI or nearest DoD component if no longer affiliated with the DON), without delay, any attempt by an unauthorized person to solicit classified information.

3. As part of a debriefing, individuals will be required to read the provisions of the Espionage Act and other criminal statutes. If individuals are retiring from active service and will be entitled to receive retirement pay, they must be advised that they remain subject to the Uniform Code of Military Justice (UCMJ).

4. As part of every debriefing (except when individuals transfer from one command to another command) a Security Termination Statement is required (paragraph 4-12 applies).

4-12 SECURITY TERMINATION STATEMENTS

1. Individuals must read and execute a Security Termination Statement (OPNAV 5511/14), exhibit 4A, at the time of debriefing, unless the debriefing is done simply because the individual is transferring from one command to another and will continue to require access to classified information.

10 MAR 1980

2. A witness to the individual's signature must sign the Security Termination Statement.
3. The command, agency, or activity's name and mailing address will be annotated on the three lines at the top of the form.
4. The original signed and witnessed Security Termination Statement will be placed in the individual's official service record or the official personnel folder for permanent retention except:
 - a. When the security clearance eligibility of a Marine is revoked for cause, the original Security Termination Statement will be forwarded by the command to the Commandant of the Marine Corps (CMC) along with a copy of the revocation letter, for placement in the Master Service Record Book (MSRB).
 - b. When the Security Termination Statement is executed at the conclusion of a Limited Access Authorization, the original will be retained in command files for 2 years.
5. If an individual refuses to execute the Security Termination Statement, the individual will be debriefed, before a witness if possible, stressing the fact that refusal to sign the Security Termination Statement does not change the individual's obligation to protect classified information from unauthorized disclosure as stated on the Classified Information Nondisclosure Agreement (SF 312). The Security Termination Statement will be annotated to show the identity and signature of the witness, if one was present, and that the individual was debriefed, but refused to sign the Security Termination Statement. Send a copy of refusals only, to CNO (N09N2).
6. The Secretary of Defense has specifically directed that Security Termination Statements will be executed by senior officials (flag and general officers, ES-1 and above, Senior Executive Service and equivalent positions). The immediate senior officials will ensure that the statement is executed and that failure to execute the statement is reported immediately to the Deputy Assistant Secretary of Defense for Security and Information Operations (DASD(S&IO) via CNO (N09N2).

4-13 TRAINING FOR SECURITY PERSONNEL

1. The NCIS Mobile Training Team (MTT) offers the Naval Security Manager's Course, DON unique core training developed to train security managers, but also available to security specialists and assistants as quotas allow. For more information on this course,

SECNAVINST 5510.30A

10 MAR 1999

contact the Atlantic MTT at NAB Little Creek, (804) 464-8925 or DSN 680-8925 or the Pacific MTT at NAS North Island, (619) 545-8934 or DSN 735-8934.

2. A Navy correspondence course entitled "Department of the Navy Introduction to the Information and Personnel Security Program," NAVEDTRA #13080, is available through the command education service officer (ESO).

3. For other security training available for DON personnel contact the CNO (N09N2) security education specialist at (202) 433-8858 or DSN 288-8858. Security training opportunities are also posted on the CNO (N09N2) Internet homepage at www.navysecurity.navy.mil.



4. CNO (N09N2) publishes the "Information and Personnel Security Newsletter" on a quarterly basis. This newsletter is also posted on the CNO homepage. The newsletter is not a directive, but states interpretations of security policies and procedures and provides advance notification of changes to the program. A roster of personnel assigned to CNO (N09N2), showing each area of responsibility is published aperiodically and posted on the homepage to assist you in routing your telephonic requests.

4-14 SECURITY AWARENESS

To enhance security, a security education program must include continuous and frequent exposure to current information and other awareness materials. Signs, posters, bulletin board notices, and Plan of the Day reminders are some of the media which should be used to promote security awareness.

10 MAR 1998

EXHIBIT 4A

SECURITY TERMINATION STATEMENT		Enter name and address of appropriate Naval or Marine Corps activity obtaining statement.
OPNAV 5511/14 (REV. 7-78) S/N 0107-LF-055-1171		
<p><u>NCIS MTT PAC</u></p> <p><u>BOX 357141</u></p> <p><u>SAN DIEGO CA 92135-7141</u></p>		
<p>1. I HEREBY CERTIFY that I have conformed to the directives contained in the Information Security Program Regulation (OPNAV Instruction 5510.1), and the Communications Security Material System Manual (CMS-4) in that I have returned to the Department of the Navy all classified material which I have in my possession.</p> <p>2. I FURTHER CERTIFY that I no longer have any material containing classified information in my possession.</p> <p>3. I shall not hereafter communicate or transmit classified information orally or in writing to any unauthorized person or agency. I understand that the burden is upon me to ascertain whether or not information is classified and agree to obtain the decision of the Chief of Naval Operations or his authorized representative on such matters prior to disclosing information which is or may be classified.</p> <p>4. I will report to the Federal Bureau of Investigation or to competent naval authorities without delay any incident wherein an attempt is made by an unauthorized person to solicit classified information.</p> <p>5. I, <u>JOHN RAY TAYLOR</u>, have been informed and am aware that Title 18 U.S.C. Sections 793-799, as amended and the Internal Security Act of 1950 prescribe severe penalties for unlawfully divulging information affecting the National Defense. I certify that I have read and understand appendix F of the Information Security Program Regulation OPNAV Instruction 5510.1. I have been informed and am aware that certain categories of Reserve and Retired personnel on inactive duty can be recalled to duty, under the pertinent provisions of law relating to each class for trial by court-martial for unlawful disclosure of information. I have been informed and am aware that the making of a willfully false statement herein renders me subject to trial therefor, as provided by Title 18 U.S.C. 1001.</p> <p>6. <input checked="" type="checkbox"/> I have not received an oral debriefing.</p>		
SIGNATURE OF WITNESS		SIGNATURE OF EMPLOYEE OR MEMBER OF NAVAL OR MARINE CORPS SERVICE (Fill in first, middle, and last name. If military, indicate rank or rate. If civilian indicate grade.)
		
TYPE OR PRINT NAME OF WITNESS LAINE S. MARQUET, LT USN		DATE 1 OCT 1998